

3.1.2. 安心とトラストに関する研究プロジェクト

□はじめに

わが国では、様々な分野で「安心・安全」が唱えられて久しい。安全とは、食品や災害のようなセーフティ(safety)に関するものから、テロ対策等の国家のナショナルセキュリティ、個人情報の漏洩（ろうえい）を守るためのネットワークやシステムのセキュリティ(security)を包含する。従来のこれらの分野では、工学的な観点から安全とされる手法を応用したシステムやサービスを提供すれば、利用者は安心するという仮定の下、研究開発が進められてきた。本研究では、この仮定に疑問を呈し、情報セキュリティ技術に対する安心感の要因や構造を明らかにしてきた。図1に示すように、安心は、安全対策に対する利用者等の主観的な感情であり、何が要因かが明確にされていない。従って、人々を安心させるにはどうしたら良いかは、実は明確ではない。多くの分野では、安全を提供すれば、人々は安心するという仮定の下、対策が議論されている。従って、提供された情報、製品、サービス、システム等が本当に安心できるものかの検証はされていない。

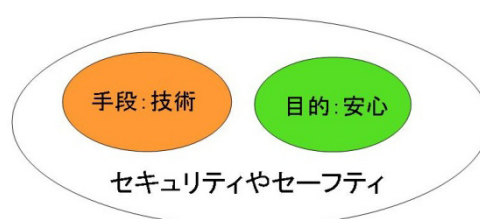


図1：安全技術(セキュリティやセーフティ)と安心感

安全工学や信頼性分野では、ヒューマンエラー回避のための技術が開発されてきたが、情報などへの不正アクセスのための攻撃を扱うセキュリティとは異なり、意図しない脅威のための技術であり、実世界のハードウェアについて主に研究されていた。しかし、最近では、セキュリティ同様、意図的な脅威を含み、高信頼性(Dependability)と呼ばれるトラストに似た複合分野として展開している。本研究では、安心の要因を明らかにすることにより、今後、人々を安心させるための情報やサービスの提供の仕方を工夫できる。今後、ユーザインタフェースをデザインする際、日本人や米国人をそれぞれ安心させる設計の提言が可能となる。本研究では、このように、古くから研究されているにも関わらず、新しい課題としてのトラストの感情部分としての安心を捉えており、そこが独創的な点である。海外でも、「Anshin」という言葉で発表している。これまで、曖昧に使われてきた「安心」の概念が明確になることにより、情報システム環境における真の安心提供についての対策を考案でき、「安心安全」な情報社会の形成に役立つと考えている。

本研究は、独立行政法人 科学技術振興機構（JST）の戦略的国際科学技術協力推進事業による「トラストと安心に関する研究」において、米国ワシントン州立大学と共同研究を2004年度より2007年度まで行い、「秀」評価を取得した。当該研究により、大学生を主に被験者対象とした質問紙調査や統計解析に基づき、安心の要因やそれらの構造を明らかにした。さらに、文献調査により、安心感と関連概念との関係も明らかにした。また、科学研究補助費の特定領域「情報爆発IT基盤」において、「ナイーブなユーザのための安全・安心情報生活空間の研究」の研究分担者として、安心についての国内のおよそ700人規模の調査を実施している。以上の研究により、情報セキュリティにおける安心についての要因を明らかにしてきた。安心の要因や構造が明確になれば、情報社会におけるシステムやサービスの安心度合いという指標を作ることも可能となる。その上で、虚偽の安心を区別できるための対策や、医療や災害等の緊急時に相手を安心させるための真の安心の応用技術について考える必要がでてきた。科学研究補助費基盤(B)研究として「虚偽の安心と真の安心に関する研究」を、2009年度より2012年度まで行っている。

以下では、トラストや安心の概念を整理して紹介するとともに、最近の研究結果についても紹介する。

ロトラストの概念

トラストについては、長らく経済学や社会学、心理学等で研究されてきた。1990年代には、コンピュータサイエンスの分野でも様々な観点で研究されるようになった。最近になり、トラストが、セキュリティやセーフティ、信頼性、プライバシー等を網羅する複合概念であることが明らかにされてきた[1][2]。他方、トラストには、客観的に計測できる認知的部分と感情部分があることをLewis等が唱え[3]、トラストの感情部分(Emotional Trust)については、電子商取引の分野で主に研究が進められてきた。本研究では、図2に示すように、安心を複合概念トラストの感情部分として捉えている。

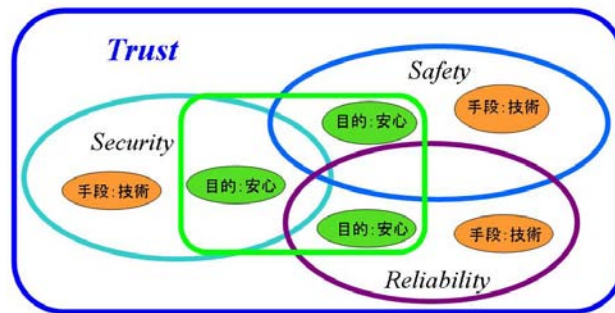


図2：トラストの感情部分としての安心

ロ安心の要因についての研究

本研究では、これまで、情報セキュリティに関する安心感について、質問紙調査と因子分析等により、その要因を分析してきた。本節では、このうち、学生425名を対象とした調査と、地方自治体職員750名程を対象とした調査について紹介する。

学生を対象とした質問紙調査

2006年10月末から11月中旬にかけ、情報系の大学生307名と非情報系の学生118名が混在した被験者を対象として質問紙調査を行った(29)。調査した結果では、安心の要因として、サービス提供に関するセキュリティ技術、サービスのユーザビリティ、利用者の経験、利用者の好み(preference)、利用者の知識、サービス提供者の信用度合の6因子が挙げられた。さらにこれらに対し、共分散構造分析を用い、安心の構造が、サービス提供者に起因する因子群(外的要因)と利用者に起因する因子群(内的要因)に分かれることが分かった。

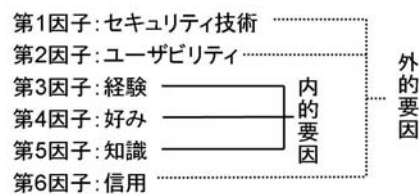


図3：学生対象の調査：因子分析結果

(最尤法, プロマックス回転)

学生の調査では、被験者が情報系と非情報系の学生が混在し、因子得点の比較から、情報系の学生は、対象となるサービスで使用されている技術に対して持っている知識を、非情報系の学生は、サービス提供者に対する信用やインタフェースに対する好みを重視していることが判明した。さらに、非情報系の学生については、内的要因に分類される因子と外的要因に分類される因子が相互に関係していることが示唆された。非情報系の学生については、被験者数が分析を行うには十分な数ではなかったため、一般の社会人の情報セキュリティに対する安心感の要因を明らかにするために、地方自治体の職員約750人を対象に質問紙調査を実施した。

社会人を対象とした質問紙調査

一般社会人として、地方自治体の職員対象の質問紙調査では、まず、予備調査(34)を、同じ自治体の109人の職員を対象に行った。その結果、被験者に回答しにくい設問項目等を修正し、750名の調査を実施した(35)。状況設定は、「インターネット上のショッピングなどのサービスを利用時に、クレジットカード番号などを入力するような場面」を想定して、安心感の根拠や理由について回答してもらった。28の設問項目を設定し、それが状況設定の場面での安心感の根拠や理由として重視するかどうかについて、かなり重視する(7点)～まったく重視しない(1点)の7段階で回答を求めた。

750名の調査では、安全性、知識、ユーザビリティ、信用、好み(プリファランス)、直感の6因子が抽出された。

第1因子の安全性は、サービス提供者側が提供するシステムの安全性に関する項目から構成され、サービスを信頼して使用できるかどうかに関する項目が多く含まれている。第2因子の知識は、被験者のセキュリティ技術に対する理解に関係するから構成され、技術だけではなく、リスクに対する理解と関係する項目も含まれている。第3因子は、ユーザビリティに関係する項目から構成され、システムの使い易さや分かり易さに関連する。第4因子は、サービス提供者に対する信用に関係し、サービス提供者の社会的信用に関する項目が含まれている。第5因子は、インタフェースのデザインに対する、個々のユーザの趣味嗜好と関係する項目が含まれている。第6因子は、根拠が不確かであるが、これまでの経験などからの直感的な印象に関係する項目で構成される。

学生と社会人の調査結果の比較

学生の調査と地方自治体職員の調査から抽出された因子の違いを比較する。ただし、2つの調査では、質問の表現や質問数が異なる。因子の違いを図4に示す。社会人の調査の第1因子「安全性」は、システムの安全に使うことができることを表しており、学生に対する調査の第1因子「セキュリティ技術」に関連するものが含まれている。今回の調査の「安全性」は、技術面だけではなく、運用面を含めて安全にシステムを利用することができるかどうかを表している。

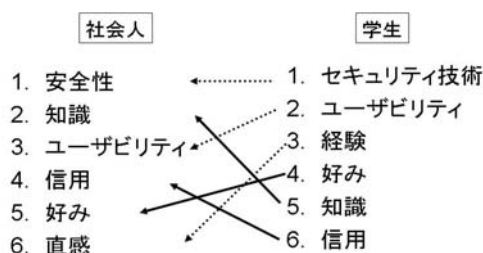


図4：社会人と学生の因子分析結果比較

(最尤法, プロマックス回転)

「知識」、「信用」、「好み」の因子については、2つの調査で同様の内容になっていた。「ユーザビリティ」の因子についても、2つ調査に共通して見られるが、今回の調査では、単に操作についてだけではなく、サービス提供者とのやりとりが親切かどうかという要素が入っている。今回の調査で抽出された「直感」の因子には、学生への調査で「経験」因子を構成していた項目を中心に、ユーザが安心を感じる根拠を論理的に説明できない要因から構成されていた。

口まとめ

トラストや安心の関連研究を紹介し、暫定的に安心をトラストの感情とする位置づけを紹介した。また、情報セキュリティに関する安心感の質問紙調査の結果を紹介し、安心の要因について説明した。

トラストに関しては、ここで紹介した以外にも、trusted computing の分野では、コンピュータ内に耐タンパ領域と呼ばれる場所を設け、ソフトウェアからの不正なアクセスができないようにするセキュリティの実践的な研究が進められている。

本研究では、この展開として、情報セキュリティについての知識のないユーザの安心感を調査した。これについては、ブレインストーミングによりユーザからの意見を収集し、KJ法を利用し、それらを整理し、質問紙を作成し直した。これを利用し、WWW上で、800名規模の調査を実施し、探索的因子分析を行った。これらの結果をさらに分析し、安心モデルを構築中である。

参考文献

- [1] Camp, L.J. "Design for Trust", Trust, Reputation and Security: Theories and Practice, ed. Rino Falcone, Springer-Verlag (Berlin) (2003)
- [2] Hoffman, L. J., et al. : Trust beyond security: an expanded trust model, Communications of the ACM, Vol. 49, No.7, pp.94-101 2006
- [3] Lewis, J. D. and Weigert, A.: Trust as a Social Reality, Social Forces, Vol. 63, No. 4, pp. 967-985 1985

3.1.3. 不快なインターフェースについての研究

本研究では、安心してインターネットを利用するために、安全でないシステムに遭遇した際に、不快を与えることにより、直感的に利用者に危険を知らせ、注意を促すインタフェースの研究調査および試作システムの開発を行った。

口はじめに

協調支援, CSCW, ヒューマンインタフェースの研究分野では、従来、利用者の使い易さを中心に考えられてきた[1]。一方、安全工学の分野では、ヒューマンエラーを回避するための対策として、手間取るインタフェースなどが考案されている。例えば、爆弾の起爆装置は二人が同時に操作しなければ動かないようになっている。医療機器では、事故を防ぐために、異なる種類の管同士が簡単に接続できないように設計されている。また、金庫は、鍵や暗証番号を二つ用意し、別の人物が管理できるようになっている。これらの知見に基づいて、本研究では、不快感をもたらすインタフェースについて探求し、情報セキュリティ技術への応用を検討する。

情報セキュリティなどの安全技術は、これまで工学的観点から、安全な技術を提供すれば利用者は安心すると考えられてきた。しかし、暗号化などの技術的対策により安全性が確保されていても、一概に利用者が安心感を得ているとは言い難い。本研究では、これまで、安心感の要因を探求してきた。これを基に安心感のモデル化を進めている。安心感とシステムの安全性の関係は図5のように示すことができる。安全な技術について利用者が安心して状態と、危険な技術について利用者が不安になることは、どちらもサービスやシステム提供の際の目標である。しかし、安全な技術について利用者が不安を感じていると、その技術は利用されなくなり、利便性の問題がでてくる。逆に危険な状態であるのに利用者が安心してるとセキュリティの問題となる。前者、ユーザビリティを改善すること等で解決する。今回の不快なインタフェースは後者の問題解決のための手段となる。